A Cellular Security System

Jason MacLulich
Senior Software Architect
Endace

Proprietary and confidential : Endace Technology Ltd

Agenda

- Evolving threats in the mobile space,
- Android malware, a case-study using a real-world bot,
- The Endace Mobile Security Platform,
- POC Deployment, Results and Issues,
- Future work and Questions

Mobile Security Signalling Plane

SMS Flooding attack (GSM/UMTS)

Paging Attack (UMTS/GPRS/CDMA2000)

Dedicated Channel attack (UMTS)

- DCH starvation (Data Plane attack)
- DCH<->FACH overload (Signalling Plane attack)

Data & Control plane saturation

- Some systems being brought down by P2P traffic
- UTRAN DoS attacks and mis-planning are synonomous
- ie : Telecom XT – System saturation
- ie : AT&T iPhone blog – planned DoS attack

Proprietary and confidential : Endace Technology Ltd

Mobile Security

Mobile security is a new problem but growing fast

Radio folk do not understand security

Security folk do not understand radio ("Mind the gap")

Attackers are learning fast – the worst yet to come

UTRAN signalling saturation the big threat

Mobile CSO needs tools to cover a wide responsibility

Network Infrastructure Protection

Fraud, LI, LEA, & Nat security engagement

User & privacy protection

And no Mobile security industry to work with

Proprietary and confidential : Endace Technology Ltd

Mobile Security Issues

- Identity theft/spoofing, billing attacks,
- Difficult to get the information to easily service warrants,
- Difficult to detect and investigate fraud,
- Infrastructure DoS attacks, RAN: SIM flooding (GSM), Resource Starvation (CDMA2000, UMTS),
- Convergence of traditionally separate circuit switched (CS) planes and data planes (PS) to IP (VoIP, VoLTE), “traditional IP attacks” such as SYN flooding, teardrop attacks, are becoming easier to use,

Proprietary and confidential : Endace Technology Ltd

Botnets Architecture & Lifecycle

- Bot is distributed/infects hosts through social engineering, email, VoIP, web sites, compounded by poor patching (OTA),
- Command and Control (C&C) required for coordinating attacks and distributing exploits:
  - Centralized (IRC, HTTP), IRC usually blocked by firewalls, HTTP easier to bypass firewall restrictions,
  - P2P (Overnet), used by the Storm bot,
  - Randomized,
- Anomalous network traffic and data patterns can be detected:
  - IRC, HTTP, DNS, Netflow anomalies

Android Exploit Surface

- Similar Linux exploit vectors, android builds on the traditional Linux kernel,
  - Linux permission model, uid, gid,
  - Linux kernel,
  - udev, webkit, OpenGL, SQlite, ARM

- "Unfamiliar" software stacks include:
  - ADB (Android Debug Bridge),
  - Binder IPC, Ashmem (Anonymous Shared Memory),
  - Dalvik VM, Zygote, Telephony stack

Android Exploit Vectors

- Initial access to the device is established remotely:
  - Through the browser (webkit),
  - Through a malicious market application (DroidDream),
  - Through an exploit against the telephony stack, including VoIP clients (SIP/RTP stack) and VoLTE implementations,
  - Through an exploit against SMS/MMS handling,

- Rooted through traditional and platform specific exploits,

- Credentials, phone books, email, SMS can be retrieved and uploaded,

- VoIP conversations can be recorded and uploaded,

Android - DroidDream

- Android marketplace malware, repackaged in a variety of different applications (Super Guitar Solo),
  - Symantec reported a total of 52 infected apps published,
  - Between 50,000 to 200,000 downloads of infected apps before they were pulled from the Android market,
  - Binaries contain the string “CVE-2010-EASY Android local root exploit (C) 2010 by 743C”,

- DroidDream, a bot, exploited two well known exploits: “exploid” and “rageagainstthecage”,
  - Exploid: Android <= 2.1 exploited lack of message authentication,
  - RageAgainstTheCage: Android <= 2.2, setuid exhaustion attack.

Android - DroidDream

- Requires the user to trigger the exploit,

- “Dials” home using a HTTP POST reporting the users IMSI and IMEI,

- Attempts to gain root privileges using exploid and rageagainstthecage,

- After a successful root installs the APK DownloadProviderManager.apk which periodically dials home and listens for commands and uploads more privileged information,

- C&C occurs over the 3G Gn link, or S5/S8 in LTE

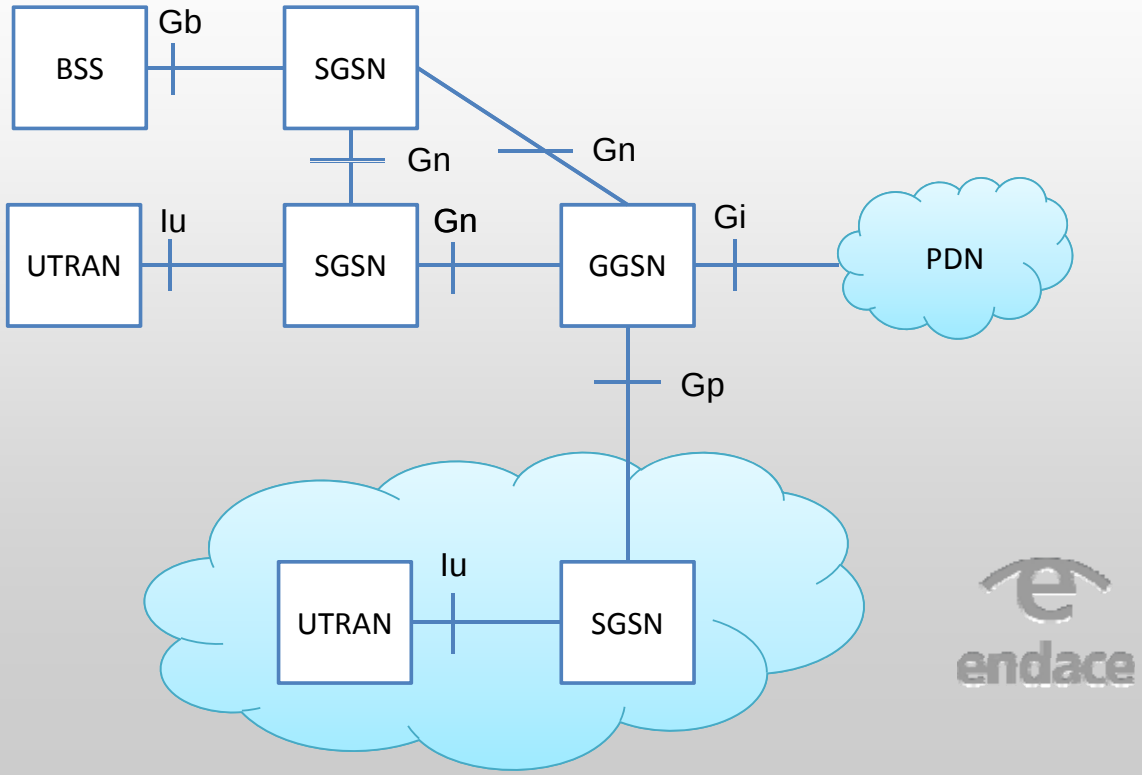
Android - DroidDream

- Classic HTTP bot can be detected by anomaly detection and signature based packet matching,
- C&C updates and downloads can be short and erratic, bursty, does not typically mimic user interaction, might be flared with “weird” NetFlow, but may give false +vs,
- alert tcp $HOME_NET any -> $EXTERNAL_NET 8080 (msg:"ET MOBILE_MALWARE Android Trojan DroidDream Command and Control Communication"; flow:established,to_server; content:"POST"; http_method; content:"/GMServer/GMServlet"; nocase; http_uri; content:"|0d 0a|User-Agent|3a| Dalvik"; http_header; classtype:trojan-activity; sid:2012453; rev:2;)

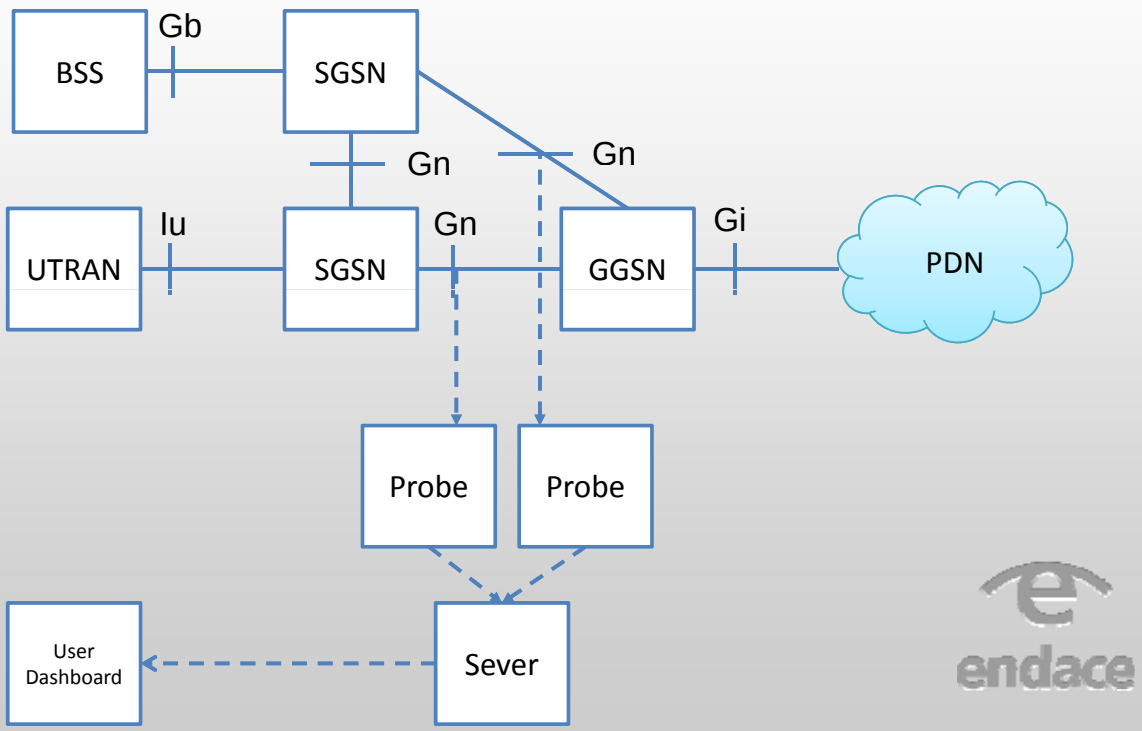
Mobile Security Platform (MSP) Focus

- Detect IP based data plane anomalies over “traditional” attack avenues, web, IM, C&C, etc..,
- Provide anomaly detection (NetFlow), signature matching (SNORT), CDR (Call Data Records) for MS (Mobile Subscriber) matching, full packet capture for analysis and user plane analytics,
- Operates over 2.5G/3G and will scale/evolve naturally to provide similar protection to “4G” LTE,
- Will scale to handle large control plane (GTP-C) updates across multiple SGSN/GGSNs,
- Will scale to handle large data plane (GTP-U) pipes.

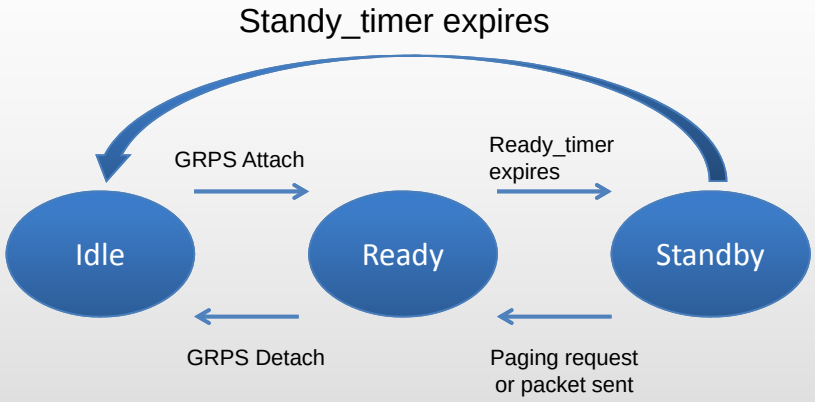
Where we sit in a 3G/UMTS/GPRS network



Where we sit in a 3G/UMTS/GPRS network

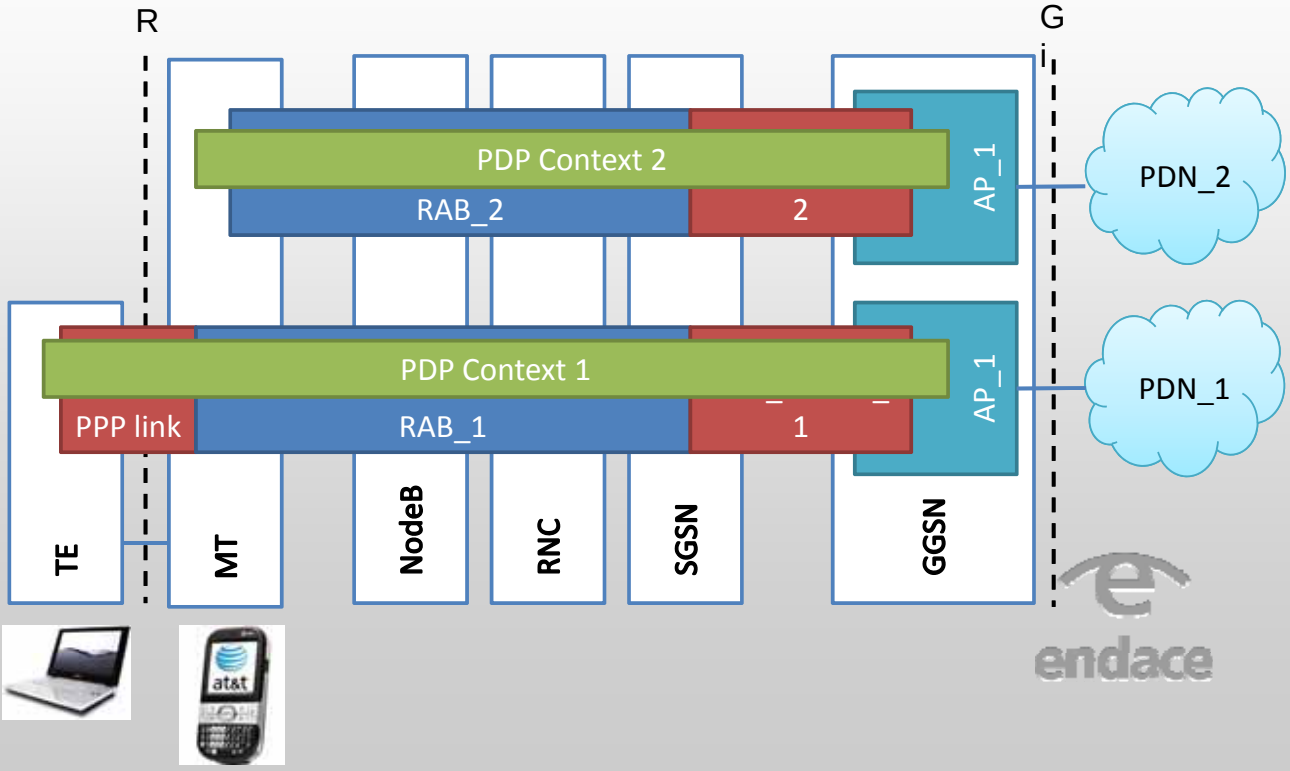


Mobile Attach

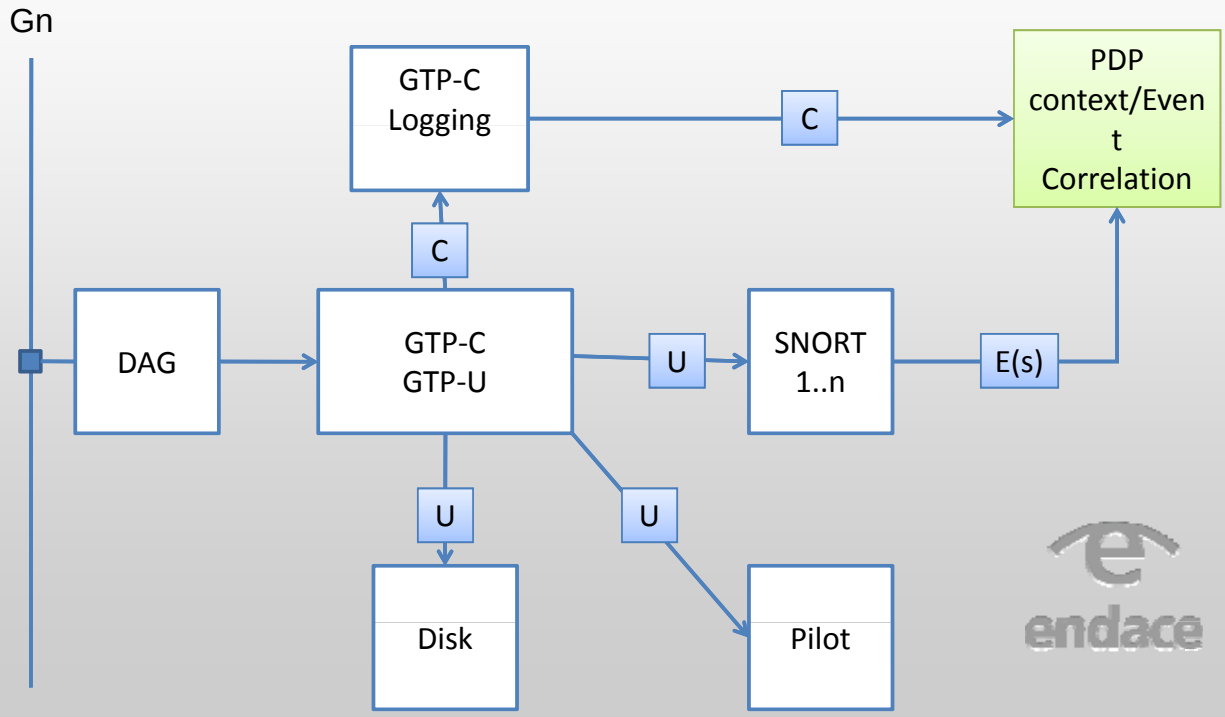


- GPRS Attach procedure triggers authentication, routing update (HLR),
- On successful GPRS Attach, PDP Context activation procedure is triggered,
- After successful PDP Context activation procedure MS is assigned an IP address.

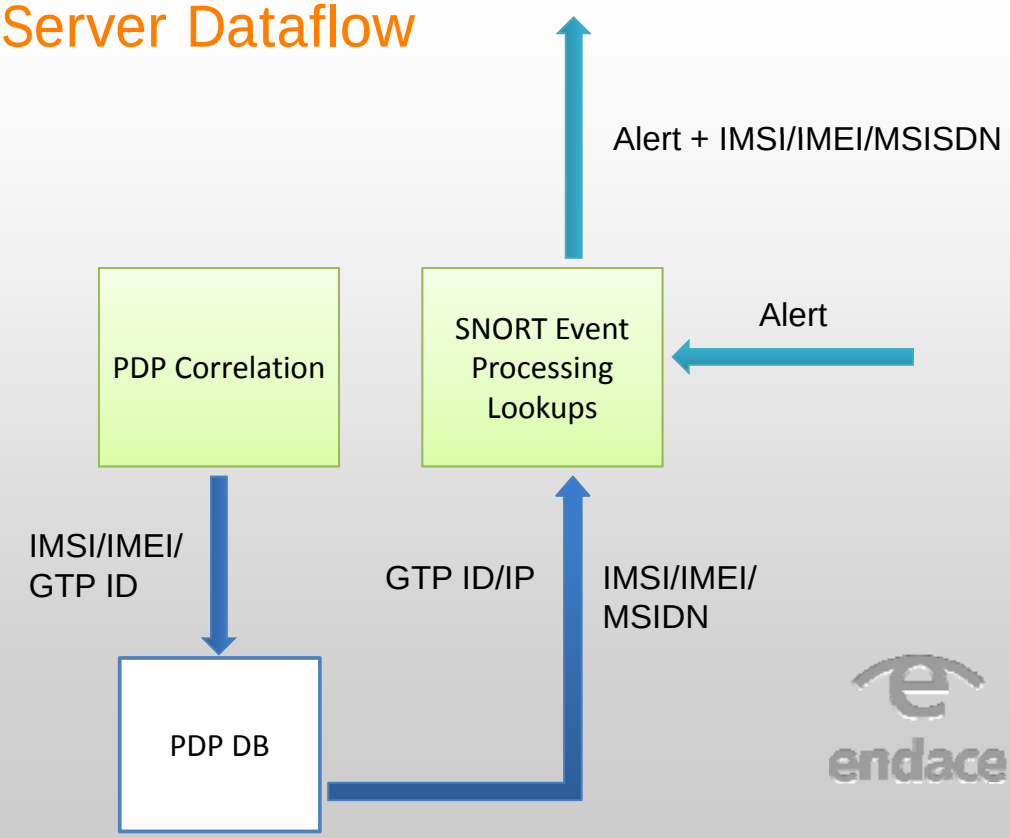
The PDP Context



MSP Probe Dataflow



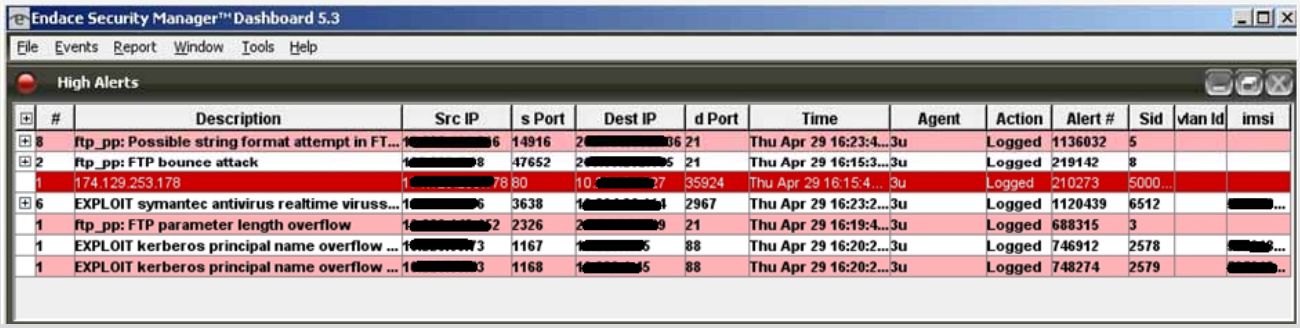
MSP Server Dataflow



MSP POC Breakdown

- Probes tap the Gn link by attaching to a SPAN port on the GGSN,
- All GTP-U/C packets stored to disk for forensics,
- All GTP-U packets de-fragmented and de-tunneled to IDS and network analytics,
  - GTP tunnel identifiers packed into packets as metadata to allow reverse mapping from Alert → GTP Tunnel,
- GTP-C packets are forwarded to the Server for PDP Correlation/Tracking/Reporting/Storage,
- Server maps from SNORT alert → { GTP-U session, GTP-U data storage }

MSP User Dashboard



#	Description	Src IP	s Port	Dest IP	d Port	Time	Agent	Action	Alert #	Sid	vlan Id	imsi
8	ftp_pp: Possible string format attempt in FT...	[redacted]	14916	[redacted]	21	Thu Apr 29 16:23:4...	3u	Logged	1136032	5		
2	ftp_pp: FTP bounce attack	[redacted]	47652	[redacted]	21	Thu Apr 29 16:15:3...	3u	Logged	219142	8		
1	174.129.253.178	[redacted]	80	[redacted]	35924	Thu Apr 29 16:15:4...	3u	Logged	210273	5000...		
6	EXPLOIT symantec antivirus realtime viruss...	[redacted]	3638	[redacted]	2967	Thu Apr 29 16:23:2...	3u	Logged	1120439	6512		[redacted]
1	ftp_pp: FTP parameter length overflow	[redacted]	2326	[redacted]	21	Thu Apr 29 16:19:4...	3u	Logged	688315	3		
1	EXPLOIT kerberos principal name overflow ...	[redacted]	1167	[redacted]	88	Thu Apr 29 16:20:2...	3u	Logged	746912	2578		[redacted]
1	EXPLOIT kerberos principal name overflow ...	[redacted]	1168	[redacted]	88	Thu Apr 29 16:20:2...	3u	Logged	748274	2579		[redacted]

MSP POC Results

- Successfully handled processing fragmented Gn links with > 3Gbps peak bandwidth and up to 1200 PDP Correlations per second, scales to 10Gbps,
- Tracks the attach/detach/update of 00000's of users hourly handled by 3 GGSNs, translating to 0000000's of PDP messages,
- Successfully map the IPs of compromised hosts to MS IMSI/IMEI/MSISDN,
- Wrote SNORT rules to track spyware, such as Flexispy, Mobilespy, and track new iPad1 users.
- Store CDR data over time to allow the detailed tracking of users over time for forensics.

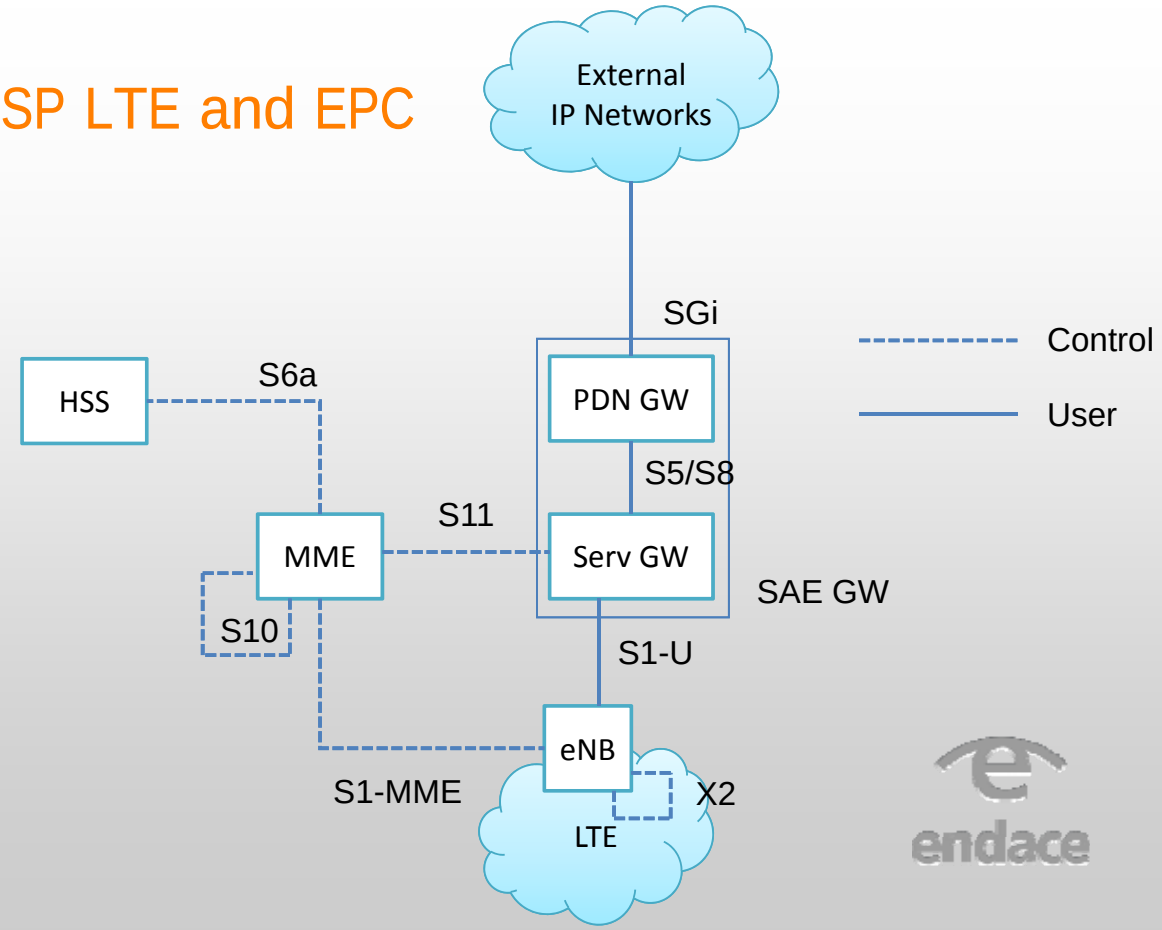
MSP POC Issues

- Gn tunnel IP fragmentation – large amounts of fragmentation came from incorrectly configured MTU sizes on the SGSN and from roaming sources over the GSN,
- Vendor specific timeouts on GSNs may cause problems if deployment is not tuned, PDP Contexts may linger,
- 3G Direct Tunnel (DT) CN optimization for HSPA, used to reduce latency by bypassing the SGSN for user-plane traffic, results in increasing the bandwidth utilization at the tap point, resource constraints are hit faster,
- Stale PDP Contexts may be preserved during any downtime.

MSP Future Work

- Migration to LTE and Evolved Packet Core (EPC)
- Extensions for Lawful Intercept (LI),
- Extensions to IPFix and NetFlowv9 to GTP embed metadata,
- Migration to Endace DOCK Platform,
- Introduce redundancy and high availability.

MSP LTE and EPC



MSP LTE and EPC

	GPRS		EPS	
RAN	UTRAN	NodeB	E-UTRAN	eNodeB
		RNC		
CN	SGSN			
	GGSN			
	Control Plane	SGSN	Control Plane	MME
		GGSN		
	User Plane	SGSN	User Plane	Serving GW, PDN GW
		GGSN		
Procesure				

MSP LTE and EPC

- EPS Bearer serves a similar purpose as the PDP Context in GERAN/UTRAN networks.
- EPS Bearer uniquely identifies traffic flows that receive a common QoS treatment between a UE and PDN GW for GTP-based S5/S8,
- One EPS Bearer is established when the UE conects to PDN,
- There is a 1 – 1 mapping between an EPS bearer and a PDP Context.

Questions?

Proprietary and confidential : Endace Technology Ltd

Thank you

Proprietary and confidential : Endace Technology Ltd

Appendix A
Mobile Security issues

Proprietary and confidential : Endace Technology Ltd

Security Issues

Network saturation (Much publicised)
Networks down (Google for NZ Telecom XT)
P2P can bring down RNCs
Increasing opportunity awareness from organised crime
Difficult to get the information to easily service warrants
Difficult to detect and investigate Fraud
Lack of detailed context based CDRs
Power constraints limit handset based protection
Traditional security tools don't work – IP centric
Need mobile security tools – IMSI/IMEI centric
Not just IDS...CDRs, and forensics tools

Proprietary and confidential : Endace Technology Ltd

Appendix B
Mobile Security Platform Design

Proprietary and confidential : Endace Technology Ltd

MSP : Long term plans

- Start with G_n interface for PoC and first release
  - Track active contexts
  - Map IP addresses to mobile ID (IP<->IMSI/IMEI)
- Later, move towards UTRAN monitoring signalling planes
  - UMTS interfaces (I_{ub} , $I_{u\text{-}ps}$, I_{ur})
  - Complicated protocol stack-ups
  - This is where Infrastructure DoS attacks will take place
  - Similar problem to mal-dimentioned infrastructure

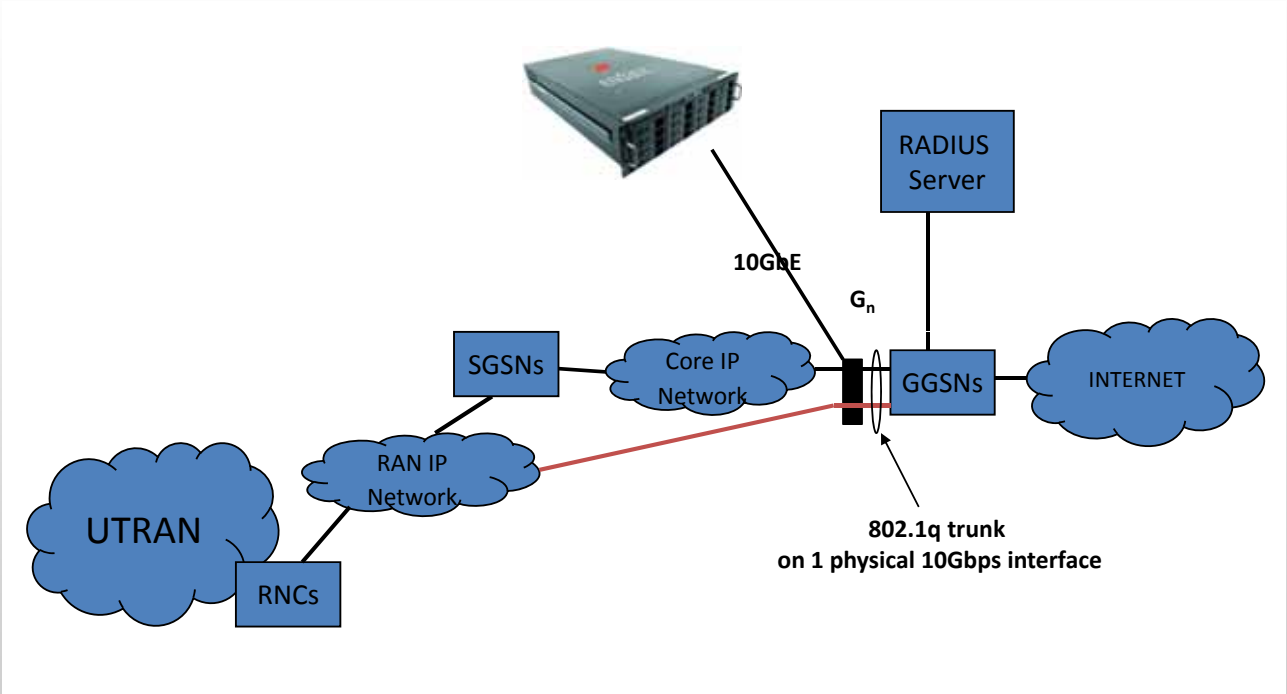
Proprietary and confidential : Endace Technology Ltd

MSP Gn PoC : Overview

- Gn Interface is tunnelled using GTP
- IP address changes with each new PHP context
- IDS events need to map Handset SIM by IMSI
- Event information needs to contain IMSI address
- At this stage, only IP traffic is inspected for threats
- Includes all network element traffic (no IMSI)

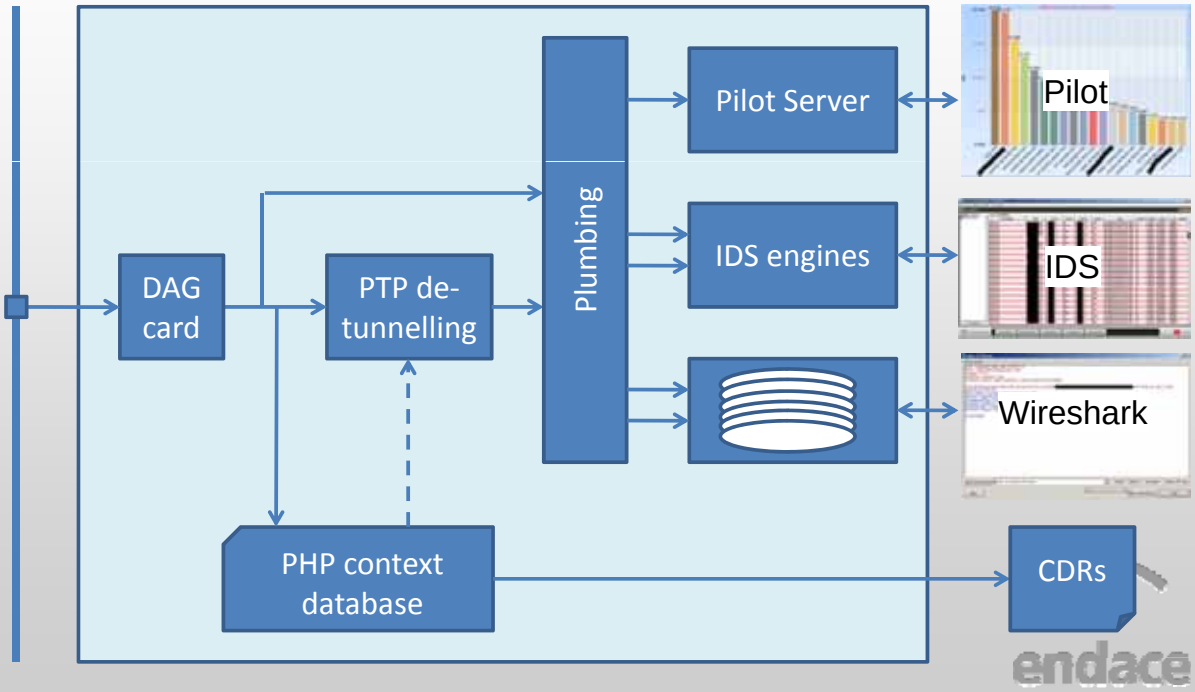
Proprietary and confidential : Endace Technology Ltd

MSP G_n : Position in UMTS Network



Proprietary and confidential : Endace Technology Ltd

MSP : Architecture



Further Extensions for discussion

- UTRAN monitoring/IDS
- Lawful Intercept (via Endace LI Applications)
- Complex CDRs –> NetFlow like Extensions
- Mining of stored data by context (IMSI, IMEI, time)
- Reasonable straight forward, but work and customer interaction required to properly define subsequent releases

Appendix C
Mobile Security Platform
CDR examples

Proprietary and confidential : Endace Technology Ltd

MSP : CDR Results

- We have several CDR output formats
- These are just 2 that we grabbed during the trial
- Happy to discuss CDR formats that are useful to you

Proprietary and confidential : Endace Technology Ltd

MSP : Tunnel context output

id	sgsnTeid	ggsnTeid	sgsnIpId	sgsnIp2Id	ggsnIpId	ggsnIp2Id	nsapi	linkedNsapi	imsi	ptmsi	euaId	msisd	seqNo	state
640242	616300150	1877338208	16		2		5		XXXXXXX08511771		79404			ok
462756	513197723	-1523667312	29		9		5		XXXXXXX09411457		65662			ok
578862	1008353830	-1519231520	1		9		5		XXXXXXX34287586		71750			ok
25063	330639910	-1525709216	18		9		5		XXXXXXX26801030		9524			ok
724430	481674619	-1518447392	3		9		5		XXXXXXX80370465		76271			ok
620359	886156014	-1518984992	5		9		5		XXXXXXX52182092		77585			ok
384592	529833964	-1524014048	3		9		5		XXXXXXX77131675		1200			ok
558630	729661735	1876478800	7		2		5		XXXXXXX23608375		58439			ok
524917	686895178	-1523392448	33		9		5		XXXXXXX42872959		62203			ok
326217	751926489	-1524258400	33		9		5		XXXXXXX77371698		7405			ok
45089	594701869	-1525600976	5		9		5		XXXXXXX00671413		16547			ok
355429	494332610	-1524139136	1		9		5		XXXXXXX00300074		29955			ok
250379	257603800	-1524574864	4		9		5		XXXXXXX00436777		37177			ok
535638	594802597	-1523345632	16		9		6		XXXXXXX00763686		23247			ok
551812	257364845	-1523277968	7		9		5		XXXXXXX42471493		11017			ok
554443	635215864	-1523266816	5		9		5		XXXXXXX29609336		42862			ok
562861	284738351	-1523229952	7		9		5		XXXXXXX34386243		11126			ok
33331	123130517	-1525663504	29		9		5		XXXXXXX81420452		12509			ok
559911	248699677	1876584176	4		2		5		XXXXXXX37462030		65174			ok
477430	706475393	-1525698096	25		9		5		XXXXXXX27500267		10418			ok

Proprietary and confidential : Endace Technology Ltd

MSP : IMSI / IP context output

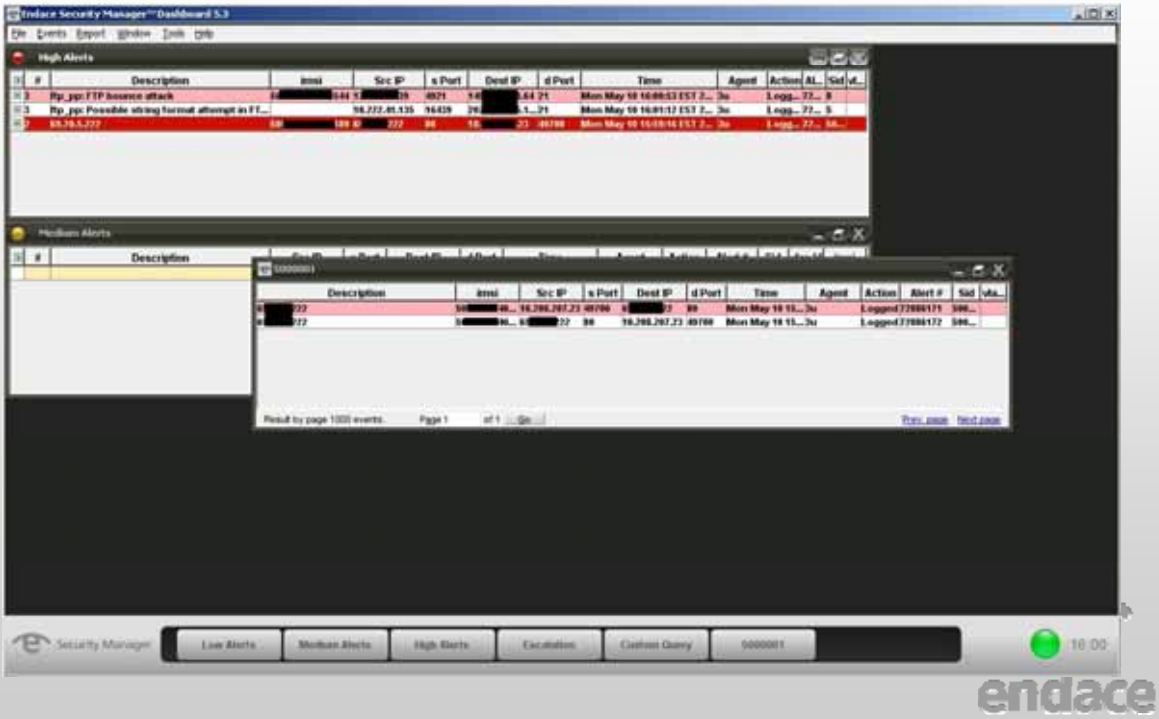
IP address	IMSI
10.222.52.168	XXXXXXX80260427
10.129.79.118	XXXXXXX33811935
10.204.8.20	XXXXXXX36550971
10.222.204.34	XXXXXXX21041256
10.222.34.27	XXXXXXX03476453
10.220.137.213	XXXXXXX37478174
10.129.24.236	XXXXXXX80415756
172.31.67.135	XXXXXXX32998482
58.165.39.152	XXXXXXX33398104
10.235.4.22	XXXXXXX36875369
10.208.98.74	XXXXXXX03076845
10.224.0.112	XXXXXXX34584048
10.1.105.220	XXXXXXX33010956
10.222.27.93	XXXXXXX40000337
10.129.145.85	XXXXXXX42145586
10.1.65.109	XXXXXXX08113017
10.2.11.117	XXXXXXX41335884

Proprietary and confidential : Endace Technology Ltd

Appendix D
Mobile Security Platform
PoC IDS example screenshots

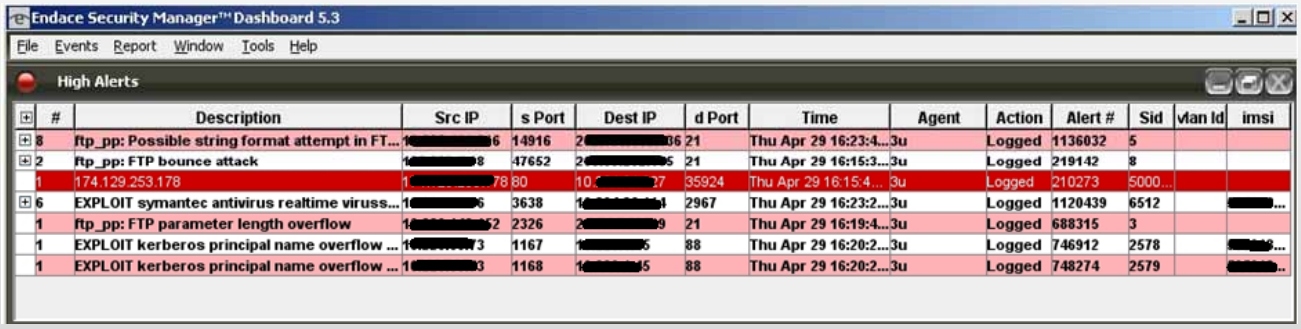
Proprietary and confidential : Endace Technology Ltd

Examples of IDS Mobile alerts on Gn traffic



Proprietary and confidential : Endace Technology Ltd

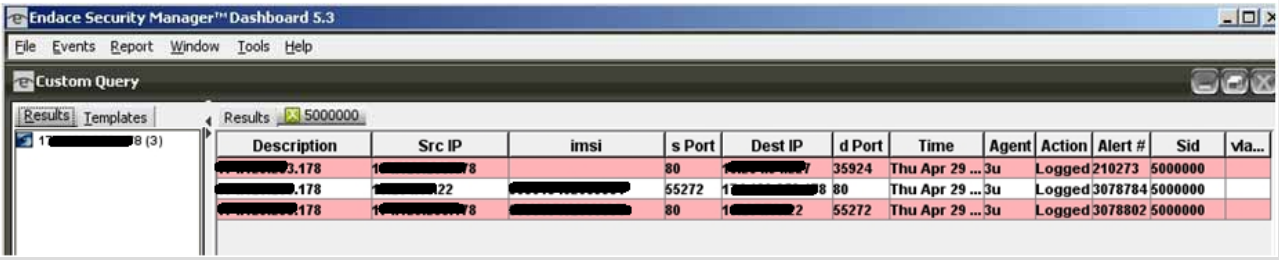
High priority IDS alerts with IP & IMSI addresses



#	Description	Src IP	s Port	Dest IP	d Port	Time	Agent	Action	Alert #	Sid	vlan Id	imsi
8	ftp_pp: Possible string format attempt in FT...	[redacted]	14916	[redacted]	21	Thu Apr 29 16:23:4...	3u	Logged	1136032	5		
2	ftp_pp: FTP bounce attack	[redacted]	47652	[redacted]	21	Thu Apr 29 16:15:3...	3u	Logged	219142	8		
1	174.129.253.178	[redacted]	80	[redacted]	35924	Thu Apr 29 16:15:4...	3u	Logged	210273	5000...		
6	EXPLOIT symantec antivirus realtime viruss...	[redacted]	3638	[redacted]	2967	Thu Apr 29 16:23:2...	3u	Logged	1120439	6512		[redacted]
1	ftp_pp: FTP parameter length overflow	[redacted]	2326	[redacted]	21	Thu Apr 29 16:19:4...	3u	Logged	688315	3		
1	EXPLOIT kerberos principal name overflow ...	[redacted]	1167	[redacted]	88	Thu Apr 29 16:20:2...	3u	Logged	746912	2578		[redacted]
1	EXPLOIT kerberos principal name overflow ...	[redacted]	1168	[redacted]	88	Thu Apr 29 16:20:2...	3u	Logged	748274	2579		[redacted]

Proprietary and confidential : Endace Technology Ltd

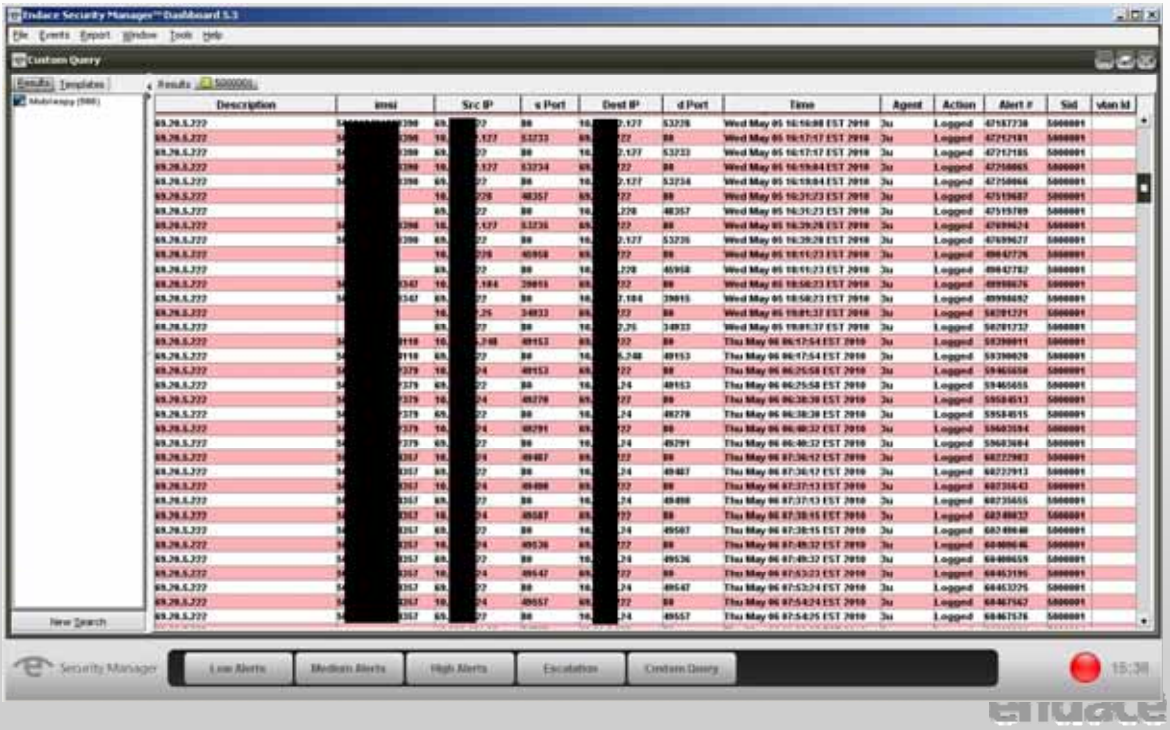
IDS Alert detail including IMSI



Description	Src IP	imsi	s Port	Dest IP	d Port	Time	Agent	Action	Alert #	Sid	vla...
[redacted].178	[redacted]		80	[redacted]	35924	Thu Apr 29 ...	3u	Logged	210273	5000000	
[redacted].178	[redacted]	[redacted]	55272	[redacted]	80	Thu Apr 29 ...	3u	Logged	3078784	5000000	
[redacted].178	[redacted]	[redacted]	80	[redacted]	55272	Thu Apr 29 ...	3u	Logged	3078802	5000000	

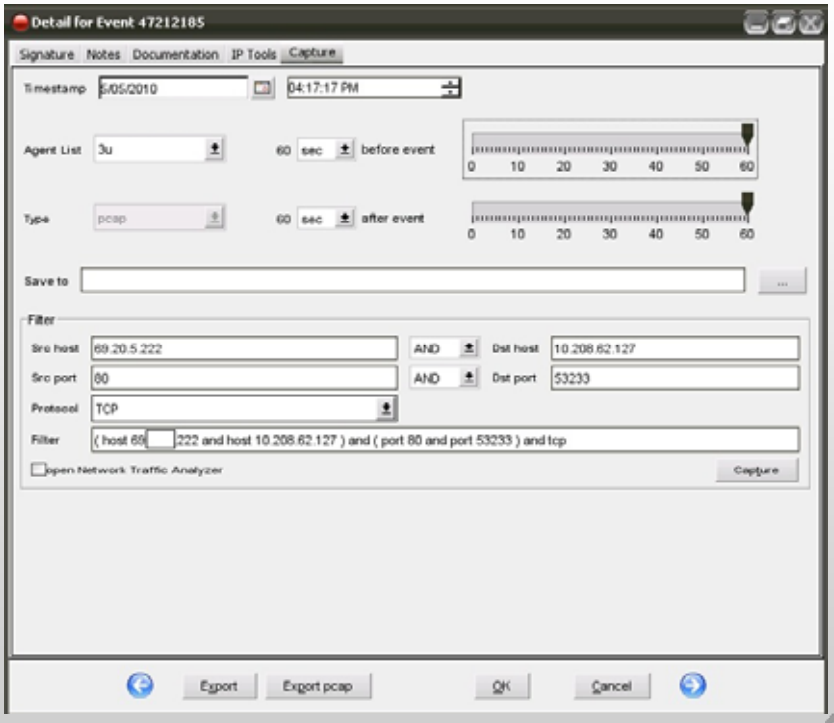
Proprietary and confidential : Endace Technology Ltd

Detecting Spyware (1 : Write a SNORT rule)



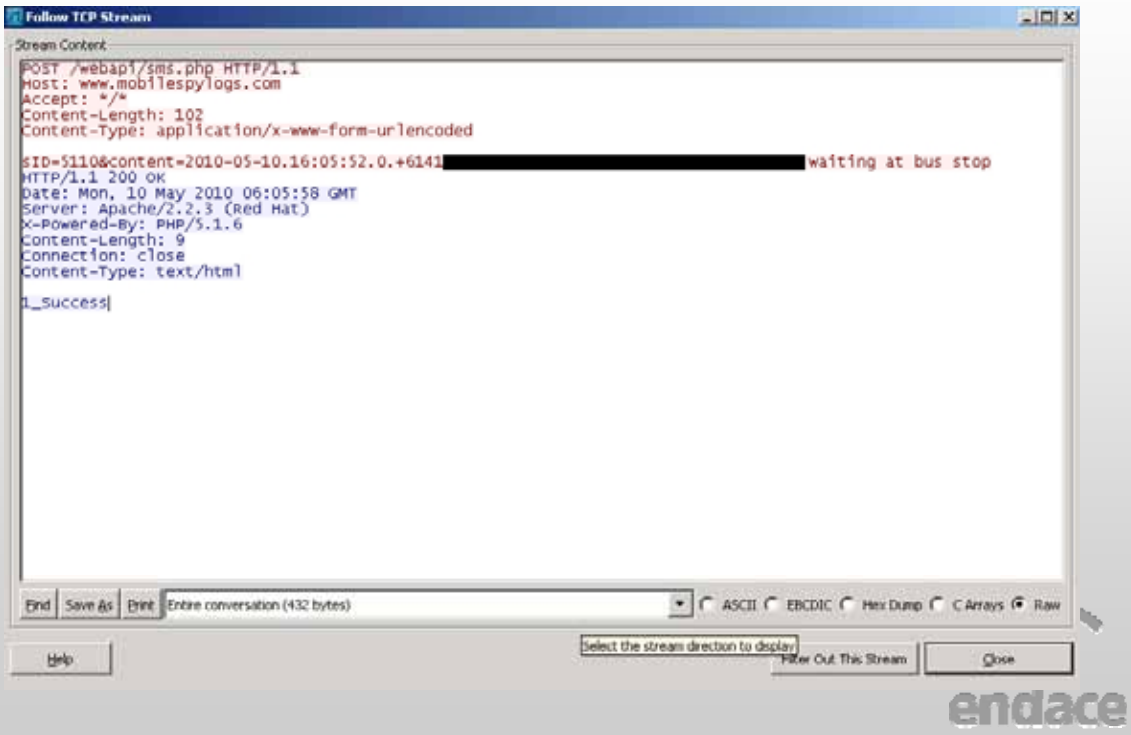
Proprietary and confidential : Endace Technology Ltd

Detecting Spyware (2 : Grab the data)



Proprietary and confidential : Endace Technology Ltd

Detecting Spyware (3 : Look at the traffic)



Appendix E
Mobile Security Platform PoC Network Analytics screenshots

endace

Mobile Security Platform : Pilot Results

- Pilot tool is used to analyse Network traffic
- In this case, de-tunnelled traffic goes to Pilot
- Able to look at all views that Pilot can provide
  - Bandwidth over time, rankings, top servers etc
  - Examples follow

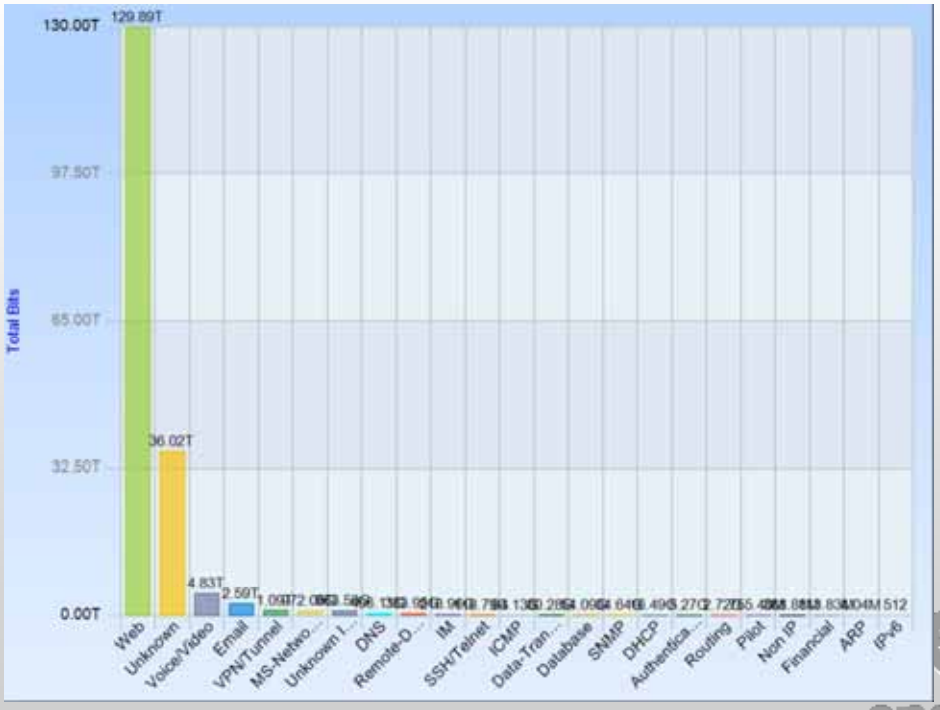
Proprietary and confidential : Endace Technology Ltd

MSP/Pilot : Bandwidth over time (bits/sec)

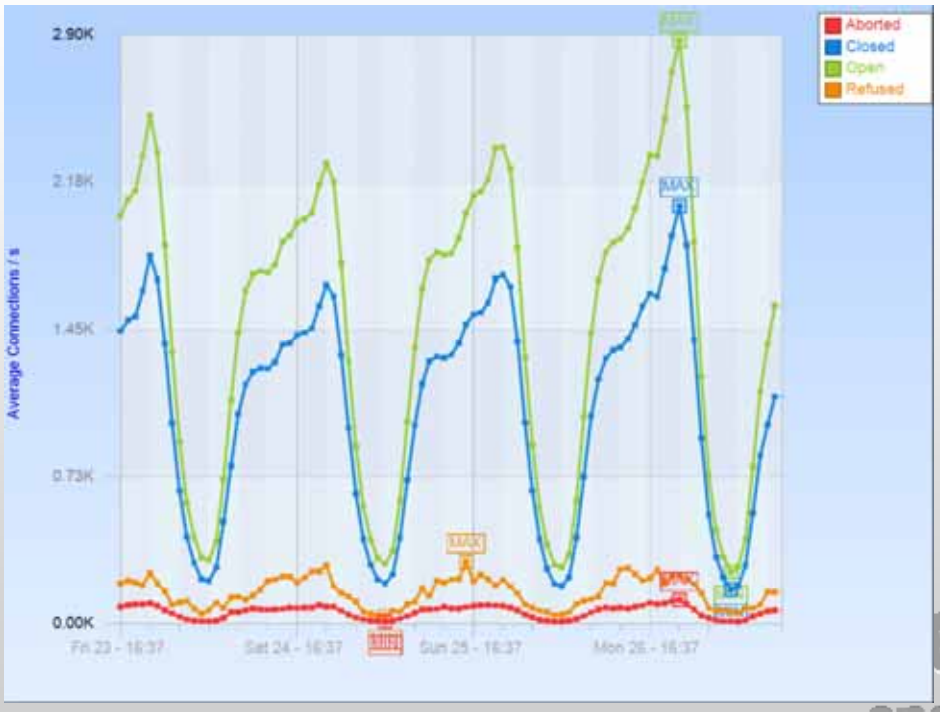
Proprietary and confidential : Endace Technology Ltd

MSP/Pilot : Traffic type over time

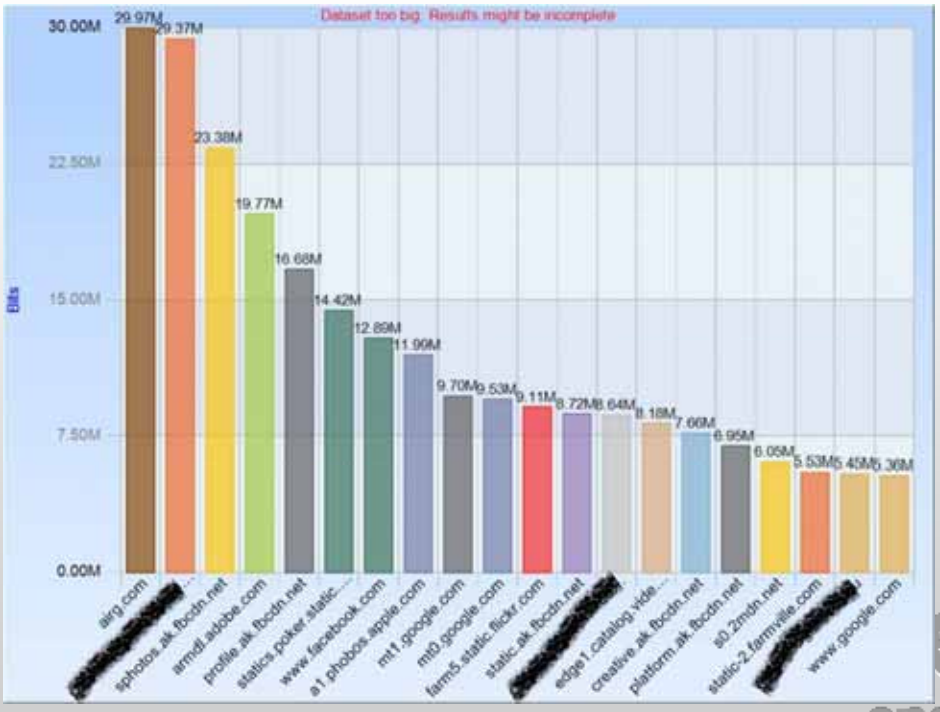
MSP/Pilot : Traffic type by rank



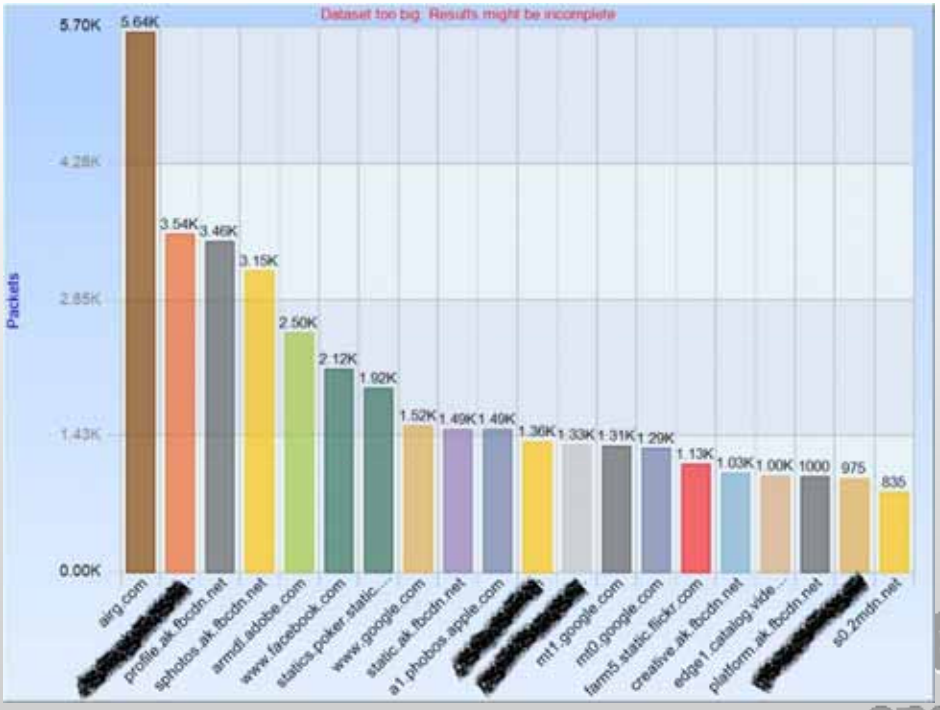
MSP/Pilot : TCP connection type and BW over time



MSP/Pilot : Top servers (bits/sec)

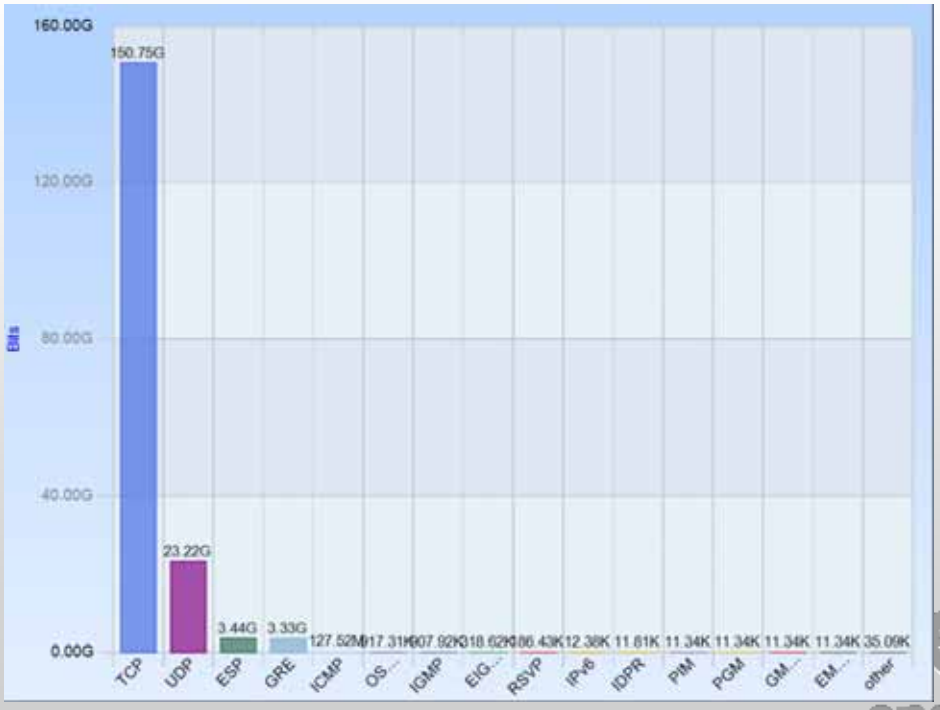


MSP/Pilot : Top servers (packets/sec)



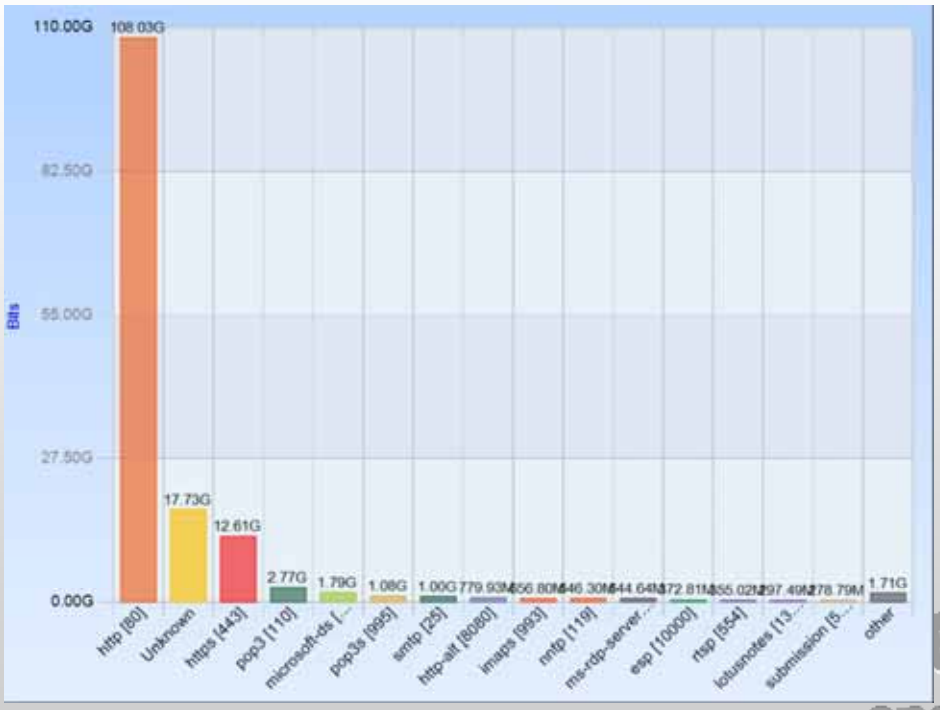
Proprietary and confidential : Endace Technology Ltd

MSP/Pilot : Traffic type (bits/sec)



Proprietary and confidential : Endace Technology Ltd

MSP/Pilot : Traffic type (bits/sec)

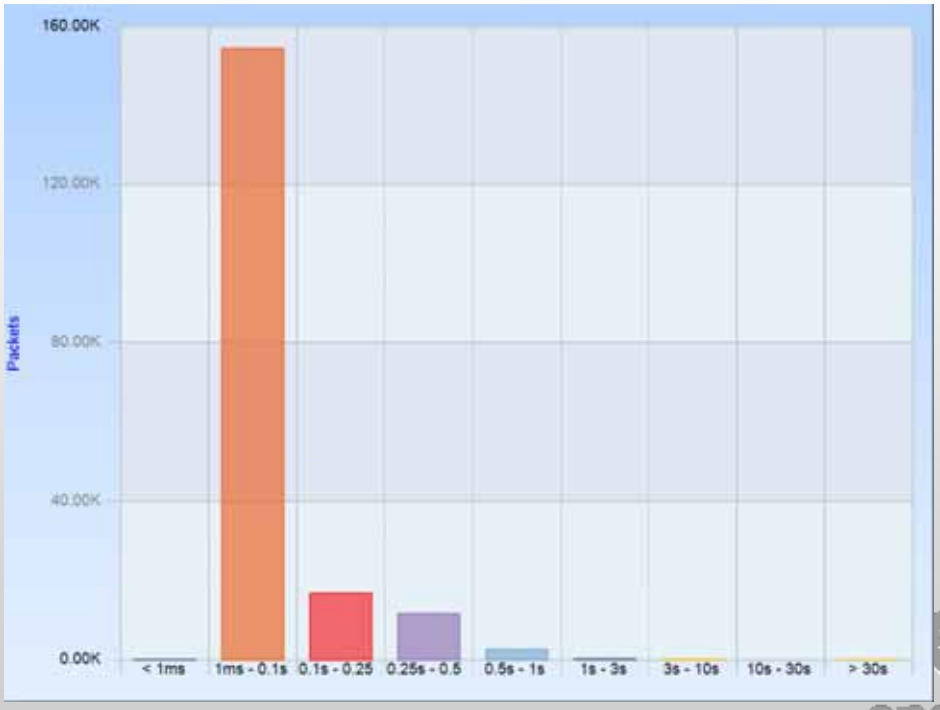


MSP/Pilot : DNS requests over time

MSP/Pilot : Top 10 DNS Destinations

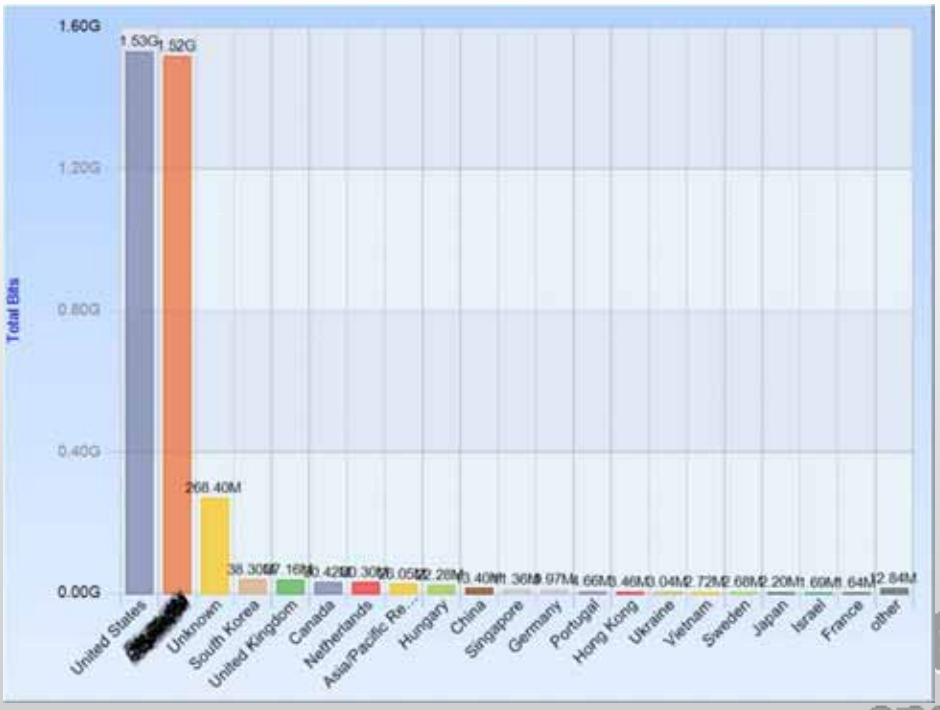
Proprietary and confidential : Endace Technology Ltd

MSP/Pilot : DNS Response times

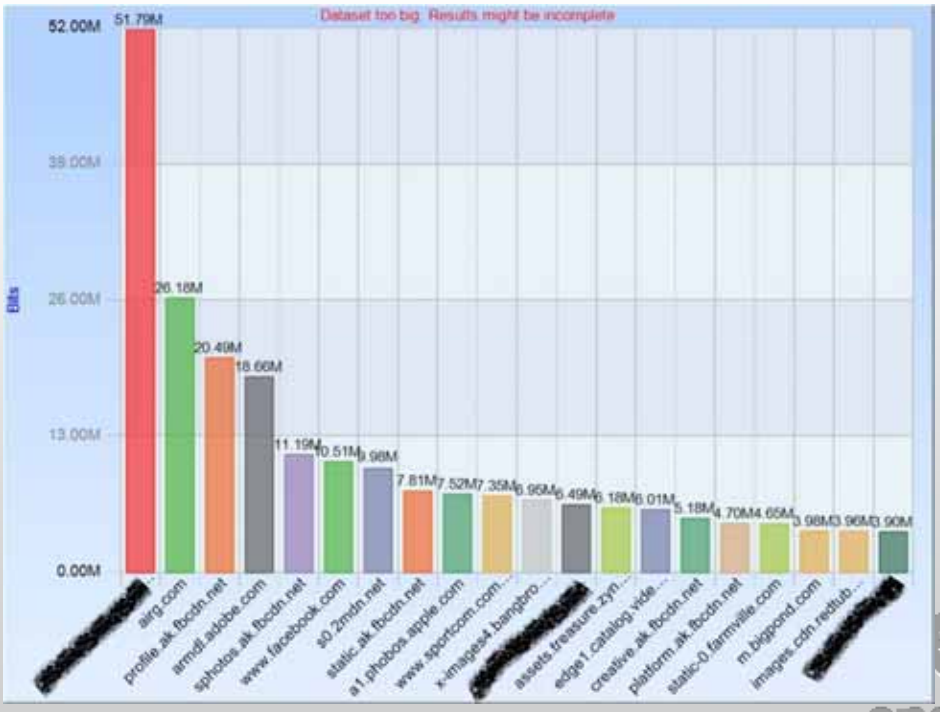


Proprietary and confidential : Endace Technology Ltd

MSP/Pilot : Top server countries



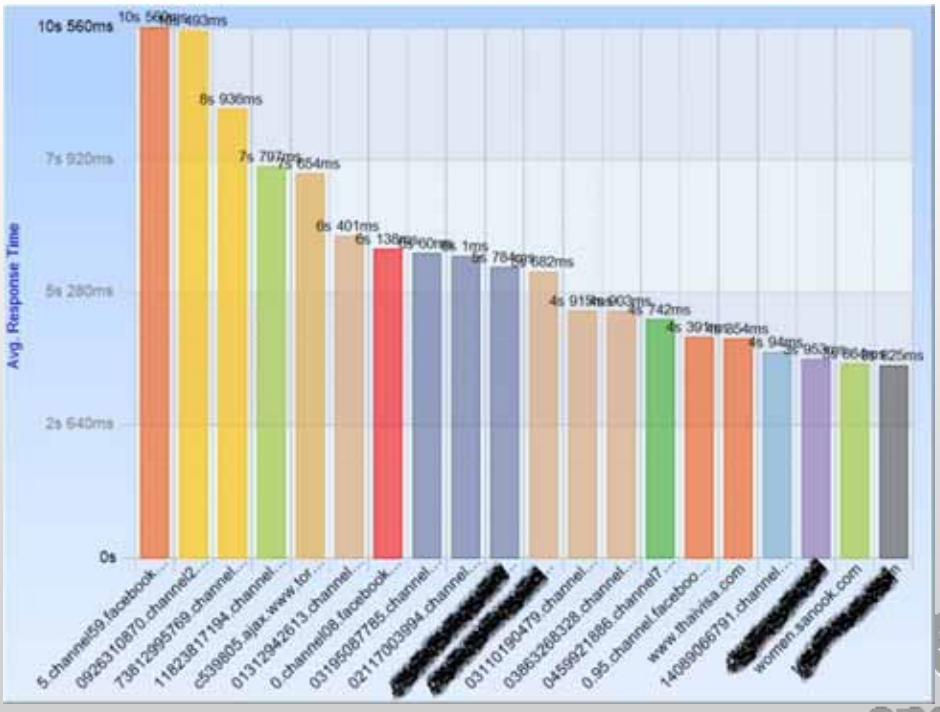
MSP/Pilot : Top server hosts



MSP/Pilot : TCP server response type bandwidth (bits/s)

endace

MSP/Pilot : Slowest servers



endace

Thank You

Stuart Wilson
CTO
stuart@endace.com
www.endace.com

endace

Proprietary and confidential : Endace Technology Ltd